

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF CHARLES E.¹ IN
SUPPORT OF DEFENDANT'S MOTION
FOR SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

¹ Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Pub. L. No. 86-36) authorizes the National Security Agency (NSA) to protect from public disclosure, among other categories of information, the names of its employees. The undersigned declarant and the NSA employee referred to in the body of this declaration occupy non-public positions with the NSA. Thus, the names of these NSA employees are referred to by first name, last initial. The Agency is prepared to provide the full name of any employee in an *ex parte*, under seal filing should the Court so require.

I, Charles E., hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746.

1. I am a Computer Forensic Examiner with the National Security Agency (NSA) and currently assigned within the Office of Counter Intelligence, Computer Forensic Investigations. I have been in this work role for approximately 2 years and have since conducted approximately 104 digital media examinations relating to security and counterintelligence issues affecting NSA and/or National Security matters. Since 2011, I have successfully completed approximately 432 training hours relevant to computer forensics, computer incident response, and network security.

2. I have been informed that the Federal Bureau of Investigation (FBI) seized a personal hard disk drive (HDD) from plaintiff Diane Roark and created a raw image copy, which was provided to me for forensic analysis. Prior to the start of analysis, I utilized the EnCase Forensic, Version 6.18.1.3, software to verify the file integrity of all images by confirming the MDS hash values were consistent with acquisition values documented by the FBI Computer Analysis and Response Team originally tasked to image the aforementioned HDD. I have completed the forensic examination of the following HDD:

Drive Model: Maxtor 6L040J2, DD Image Files Labeled: Q3_1_2.00X Serial: 662200214659
Cylinders: 77557 Heads: 16 Sectors: 63 Total Sectors: 78177792 Drive Size: 37.3 MD5 Value:
23F8BB82 5FADEC4B 455BD483 662D1077.

3. The scope of the forensic examination was to identify any data related to classified information or information protected by the National Security Agency Act of 1959 within the files located in plaintiff Roark's user profile on the HDD (the user profile is the directory "C:\Documents and Settings\Diane Roark"). Standard keyword terms associated with classified NSA and classified National Defense Information were used to search the foregoing user profile

directory, except for the jpg (picture) files and wav (audio) file. The keywords cannot be included in this declaration at an unclassified level, but include terms such as "NSA", "TOP SECRET", as well as terms specific to NSA activities. The initial keyword search was only conducted of the user profile directory and did not include any other directories, including the directories that appear to include more than 10,000 America On-Line (AOL) emails.

4. The initial keyword search indicated that 53 files in the user profile directory contained one or more of the keywords. I provided a copy of four of these 53 files to Miriam P., Deputy Chief of Staff for Policy and Corporate Issues for the Signals Intelligence Directorate of the NSA, for classification review.

5. Additionally, the initial keyword search did not include any search terms from the House Permanent Select Committee on Intelligence. The NSA does not have the authority to agree to the release of classified or protected information that originates from another federal agency or department. When the question of disclosure of such information arises, the NSA refers the information and the issue of disclosure to the originating agency for a decision.

6. Although there are tools and techniques designed to overwrite deleted files, various complications and/or circumstances can, and do, subvert their complete effectiveness. For example, technical issues within HDDs, such as unreadable, or "bad", sectors can prevent traditional forensic tools from accessing those areas. Also, if a user of the HDD employs any data-hiding techniques, such as encryption, locating this type of data can be difficult to discover; thus, the data would not be overwritten. I am not aware of a technical solution that completely ensures the removal of data from a HDD that does not result in the total destruction and inability to use the HDD.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 29th day of September 2014 at Fort Meade, Maryland.



CHARLES E.

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Charles E. in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

CERTIFICATE OF SERVICE